COT Security Alert – The Risk of Default Credentials

Within large scale environments, System Administrators may leave devices and other systems with default usernames and passwords. Common reasons for not disabling or modifying these credentials could be as simple as not knowing that a built-in account needs to be changed or assuming that perimeter firewalls or other security devices protect the organization from unauthorized access. This practice is unwise considering that during the initial reconnaissance phase of an attack, hackers will often follow-up their scans by reviewing the services that are running on a target – thus, providing the attacker an opportunity to research the services, download manuals, and compile lists of default credentials to either try manually or via automated tools and viruses.

When default Administrator accounts and passwords for devices and systems are overlooked, it compares to leaving your keys outside a locked door of your home and allows for easy compromise without the complexity of malicious scripts and exploits. Vendors continue to include default usernames and passwords in their products and it is the responsibility of System Administrators to ensure that the default settings of any product implemented in our environment are changed before they go into production. This is why minimum baseline configurations; password changes, complexity, and expiration are so important - especially when it comes to critical systems, devices, and environments that house sensitive data.

It is recommended that insecure configurations (factory default credentials, management interfaces hosted over insecure protocols, default services, etc) be reviewed. In order to prevent vulnerabilities, minimum baseline configurations should be in place before any device or system is placed on the network. Best practice includes the following:

- All manufacturer patches/updates should be applied where technically feasible
- Any default services that are not required should be disabled
- Factory default credentials should be changed to meet Enterprise standards (account names should be changed where possible)
- Management interfaces should be secured using encryption (ex: HTTPS, SSH, SSL) to protect authentication
- Where possible, management interfaces should used LDAP authentication

Notice: COT is providing this information so that you are aware of security threats, vulnerabilities, software patches, etc. You should consult with your network administrator or other technical resources to ensure that the appropriate actions for these alerts are followed. If you are a network administrator and need additional information, please call the Help Desk at 502.564.7576.

Security Administration Branch
Commonwealth Office of Technology
120 Glenn's Creek Road, Jones Building
Frankfort, KY 40601
COTSecurityServicesISS@ky.gov
http://technology.ky.gov/ciso/

NOTICE: COT is providing this information so that you are aware of the latest security threats, vulnerabilities, software patches, etc. You should consult with your network administrator or other technical resources to ensure that the appropriate actions for these alerts are followed. If you are a network administrator and need additional information, please call the Help Desk at 502.564.7576.

Security Administration Branch
Commonwealth Office of Technology
120 Glenn's Creek Road, Jones Building
Frankfort, KY 40601
COTSecurityServicesISS@ky.gov
http://technology.ky.gov/ciso/